REMARKS

Upon entry of this amendment, claims 1, 3-5, 7-18, 20-23, 29, 31, and 46-50 will be pending. By this amendment, claims 1, 18, 29, and 46 have been amended. No new matter has been added.

§102(a) Rejection of Claims 1, 3-5, 13, 18, 20-23, 29, 31, 46, and 47

In Section 4 of the office action dated December 9, 2010 ("the Office Action"), claims 1, 3-5, 13, 18, 20-23, 29, 31, 46, and 47 stand rejected under 35 U.S.C. 102(a) as being anticipated by Geiger et al. (U.S. Patent No. 6,463,534; hereinafter referred to as "Geiger").

Regarding amended claim 1, it now recites:

> A method of adding a client as a member of a hub network, comprising:
>
> (a) detecting a client connected to a server in a hub network;
>
> (b) authenticating the client to determine an identify of the client;
>
> (c) authorizing the client to determine that the client is a compliant device that operates according to rules defined for the hub network,
>
> (d) wherein the compliant device enables a user to present, move, and copy content data to be controlled to reflect guidelines of licenses of the content data set for a licensing authority;
>
> (e) adding the client as a member in the hub network when it is determined that the client has been detected, authenticated, authorized, and is in a local environment of the server; and

(f) providing licenses for the content data bound to the hub network to members of the hub network,

(g) wherein a source version of the content data is stored on the server, and copies of the source versions are stored on the compliant device as sub-copy versions.

(emphasis / limitation designations added)

In addition to the arguments presented in responses to previous office actions (which are maintained here), following additional arguments are presented.

Regarding limitations in (c) through (g) [limitation (d) is newly added], they recite "authorizing the client to determine that the client is a compliant device that operates according to rules defined for the hub network, wherein the compliant device enables a user to present, move, and copy content data to be controlled to reflect guidelines of licenses of the content data set for a licensing authority; adding the client as a member in the hub network when it is determined that the client has been detected, authenticated, authorized, and is in a local environment of the server; and providing licenses for the content data bound to the hub network to members of the hub network, wherein a source version of the content data is stored on the server, and copies of the source versions are stored on the compliant device as sub-copy versions."

These limitations ((c) through (g)) are disclosed in at least Paragraphs [0030], [0032], [0065], [0081], [0086]-[0087], [0090], and [0107] (of the Publication of the present application – Pub. No. 2004/0117484) as follows (emphasis added):

> [0030] … Before adding a device as a member to the hub network HN1, the PVR 105 authenticates a device, confirming the identity of the device, and authorizes an authenticated device, confirming that the device is a

compliant device. If the PVR 105 does not authenticate and authorize a device, the PVR 105 does not add that device to the hub network HN1. ...

[0032] ... The locked content data stored by the server is the source for copies of the content data in the hub network and is the "source version." Copies of the source version content data are stored on clients and are "sub-copy versions" ...

[0065] The overlapping hub networks provide a flexible environment for managing the use and copying of content. Each server manages the devices and content in the server's hub network and each client operates in compliance with the rules of the hub network. As a result, a user can present, move, and copy content data through the media network environment in a convenient manner and at the same time the presentation, copying, and moving of the content data is controlled to reflect the licensing guidelines set for a licensing authority (e.g., by the content owner). In addition, the management of each hub network is grounded in the server of the hub network.

[0081] After successfully authenticating the client device, the server receives an add request to add the client device from a user, block 1820. The server waits to proceed with adding a client device until the server receives an affirmative request from a user to add a specific client device. In another implementation, the server requests approval or confirmation from the user to add an authenticated device when the device is detected instead of waiting for a request from the user. In another implementation, the server waits to authenticate the client device until after receiving a request or approval to add the client.

[0086] In an alternative implementation, a server automatically attempts to add detected client devices upon detection, or uses a set of rules to determine when to attempt to add connected client devices. In another implementation, the server automatically attempts to authenticate and authorize detected client devices, but does not add an authenticated and authorized device as a member until after receiving a user request or approval.

[0087] In another implementation, when the device count has reached the device limit and the server is attempting to add another device, the server contacts a device registration server, such as through an external network connection. The device registration server indicates whether the client device is to be added to the hub network or not. The device registration server maintains information for hub networks and their member devices. The device registration server can use various criteria to determine whether to allow the client device to be added or not. In one implementation, the device registration server compares a threshold to how many hub networks to which the client device has already been added as a member. In another implementation, the device registration server compares the number of devices already added to the hub network to a second device limit, allowing the client device to be added if the device count is below the second device limit. ...

[0090] The server disables the licenses for sub-copy versions of bound instances bound to the server's hub network for the client device to be removed, block 1910. The server sends a disable request to the client indicating the sub-copy versions to be disabled and the client disables the corresponding licenses. In addition, the removed client device will not be able to receive a new license or be able to refresh an existing license for a bound instance bound to the hub network from which the client device was removed. In one implementation, a compliant client device automatically disables all licenses for sub-copy versions stored on the client and for bound instances bound to the hub network from which the client has been removed once the client has been removed. Removing a client from one hub network does not necessarily disable licenses for sub-copy versions for bound instances bound to another hub network.

[0107] ... In one implementation, a server can revoke a key if the server has determined the key has been compromised. In this case the server requests compliant devices disable the revoked key so that the revoked key will not be used to access secure media content.

In addressing limitation (c) of claim 1, the Office Action cites Geiger, column 10, lines 8-54. These passages of Geiger are recited here for reference:

> [Col. 10, lines 8-54] A "domain", or "security domain", is a public key infrastructure under the control of a single authority and using a defined internal naming scheme, algorithms, and policies. Domain authority flows for a domain root certification authority having a globally unique name. This allows domains to generate agreements and hook together forming a global PKI. An entity that has been enrolled in a domain by the certifying of the public key that the entity owns within the domain is a "domain member". The following are the possible WAP domains, some or all of which will be referred to: manufacturer(s); network; operator(s); wireless service provider(s); content/services providers (e.g., banking domain); trusted third party domains (e.g., an independent certification agent or authority); device owner (fleet operator domain); and device user (personal domain).
>
> An "attribute" is either a characteristic (which can be considered to be a name) or a right (i.e. a permission, for example a permission to access a purchased service). Examples of attributes, are owned objects (e.g. directories & files, hardware and & interfaces) and owned rights/permissions (e.g. make call; establish network connection; send SMS message; read/write/update files & directories; configure device hardware; access network management station.
>
> In order to implement this security infrastructure, the WAP Public Key system 10 enrolls and authenticates WAP domain members and distribute attributes. Note that the word "distribute" includes "distribute to purchaser"; i.e., subscribers may be purchasing attributes such as access to content or services.
>
> The WAP PKI architecture consists of autonomous security domains tied together by cross-certification. Such cross-certification is a part of service roaming agreements between service providers and system operators. Cross certification is the process by which two domain root CA's issue one another cross-certificates; thereby authorizing one

> another's root certificates (keys). Cross-certificates generally contain the address of one or more inter-domain validation servers and may also contain other information related to the cross-certification agreements. For the wireless industry cross-certification can be similar to creation of roaming agreements. Within a security domain the algorithms, naming scheme, and policies of that domain are determined by the owner of the domain. During the cross-certification procedure, domains agree on inter-operability issues and configure validation servers to allow certificate validation to be performed.

However, these passages fail to teach or suggest limitation (c) of claim 1. For example, although the cited passages describe concepts of domain attributes, none of the cited passages specifically teach or suggest "authorizing the client to determine that the client is a compliant device that operates according to rules defined for the hub network".

Regarding newly-added limitation (d) of claim 1, it recites that "the compliant device enables a user to present, move, and copy content data to be controlled to reflect guidelines of licenses of the content data set for a licensing authority". None of the cited passages disclose this limitation.

In addressing limitation (c) of claim 1, the Office Action cites Geiger, column 10, lines 8-54 and column 12, lines 19-31. The first passage was already recited above. The second passage is recited here for reference:

> [Col. 12, lines 19-31] Server 400 is a validation server. A validation server is a server that is configured to validate certificates for domain members. Domains that cross-certify are expected to provide accessible validation servers that obtain and validate certificate chains. This service is important when there are domains with local naming schemes. Since these schemes may not be understood by an outside domain, it is necessary for the validation service to be provided. A validation server that is configured to communicate with one or more outside domains is an inter-

> domain validation server. In addition validation servers may provide local domain validation for thin clients that are domain members but do not have the ability to obtain and validate a certificate chain on their own.

Again, these passages fail to teach or suggest limitation (e) of claim 1. For example, although the cited passages describe concepts of domain attributes and validation servers, none of the cited passages specifically teach or suggest "adding the client as a member in the hub network when it is determined that the client has been detected, authenticated, authorized, and is in a local environment of the server".

In addressing limitation (g) of claim 1, the Office Action cites Geiger, column 8, lines 28-45 and column 10, lines 8-54. The second passage was already recited above. The first passage is recited here for reference:

> [Col. 8, lines 28-45] Thus a wireless electronic commerce system has been described having a wireless gateway 18 to a wireless network 19 with which a wireless client device 11 having a unique client identifier is capable of communicating. At least one server has been described coupleable to the wireless gateway, delivering content items to the wireless device and maintaining digital content certificates for content items and digital license certificates for licenses for the content items. In the preferred embodiment the server 17 delivers the content and the CA server 15 maintains the digital license certificates. The at least one server maintains, for each wireless client associated with the system, a record of licenses for that client and a record of content items associated with each license. In other words, the CA server 15 maintains a database or list correlating wireless client IDs with licenses (or license certificates) for each client ID and content items (e.g. software products) associated with the licenses.

Again, these passages fail to teach or suggest limitation (g) of claim 1. For example, although the cited passages describe concepts of domain attributes and wireless

gateway, none of the cited passages specifically teach or suggest that "a source version of the content data is stored on the server, and copies of the source versions are stored on the compliant device as sub-copy versions".

Based on the foregoing discussions, claim 1 should be allowable over Geiger. Regarding independent claims 18, 29, and 46, similar arguments as those of claim 1 apply to these claims. Therefore, claims 18, 29, and 46 should also be allowable over Geiger. Since claims 3-5, 13, 20-23, 31, and 47 depend from one of base claims 1, 18, 29, and 46, and include all of the limitations of the base claims, claims 3-5, 13, 20-23, 31, and 47 should also be allowable over Geiger.

Accordingly, it is submitted that the rejection of claims 1, 3-5, 13, 18, 20-23, 29, 31, 46, and 47 based upon 35 U.S.C. §103(a) has been overcome by the present remarks and withdrawal thereof is respectfully requested.

§103 Rejection of Claim 7

In Section 20 of the Office Action, claim 7 stands rejected under 35 U.S.C. 103(a) as being unpatentable over Geiger, and further in view of Kamperman (U.S. Patent Publication No. 2005/0273608).

The arguments presented in responses to previous office actions regarding claim 7 are maintained here, and following additional arguments are presented.

Based on the above discussions regarding claim 1, since claim 7 depends from claim 1, claim 7 should also be allowable over Geiger.

Further, claim 7 recites:

> The method of claim 1, wherein determining that the client is a compliant device comprises
>
> sending a compliance confirmation request to the client to request information from the client to confirm that the client will abide by the rules defined for a hub network.

The Office Action states that Kamperman "discloses sending a compliance confirmation request to the client to request information from the client to confirm that the client will abide by the rules defined for a hub network" in Paragraphs 5, 6, 29-31, which are recited here:

> [0005] One way of protecting content in the form of digital data is to ensure that content will only be transferred between devices if
>
> [0006] the receiving device has been authenticated as being a compliant device,
>
> [0029] In an embodiment the common secret has been shared before performing the distance measurement, the sharing being performed by the steps of,
>
> [0030] performing an authentication check from the first communication device on the second communication device by checking whether said second communication device is compliant with a set of predefined compliance rules,
>
> [0031] if the second communication device is compliant, sharing said common secret by transmitting said secret to the second communication device.

However, the above-recited paragraphs of Kamperman merely recite "performing an authentication check from the first communication device on the second communication device by checking whether said second communication device is compliant with a set of predefined compliance rules." These paragraphs fail to teach or

suggest specifically that "a compliance confirmation request [is sent] to the client to request information from the client to confirm that the client will abide by the rules defined for a hub network." That is, in Kamperman, the first communication device merely performs authentication check on the second communication device, rather than sending a compliance confirmation request to the client to request information from the client to confirm that the client will abide by the rules defined for a hub network.

Accordingly, it is submitted that the rejection of claim 7 based upon 35 U.S.C. §103(a) has been overcome by the present remarks and withdrawal thereof is respectfully requested.

§103 Rejection of Claims 9, 10, 48, and 49

In Section 22 of the Office Action, claims 9, 10, 48, and 49 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Geiger, as applied to claims 1 and 46, and further in view of Fransdonk (U.S. Patent Publication No. 2003/0167392).

Since claims 9, 10, 48, and 49 depend from one of base claims 1 and 46, and include all of the limitations of the base claims, claims 9, 10, 48, and 49 should also be allowable over Geiger. Further, Fransdonk does not disclose any further limitations disclosed in the base claims. Therefore, claims 9, 10, 48, and 49 should be allowable over the combination of Geiger and Fransdonk.

Accordingly, it is submitted that the rejection of claims 9, 10, 48, and 49 based upon 35 U.S.C. §102(a) has been overcome by the present remarks and withdrawal thereof is respectfully requested.

§103(a) Rejection of Claims 11 and 50

In Section 27 of the Office Action, claims 11 and 50 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Geiger and Fransdonk, and further in view of Uhlik (U.S. Patent Publication No. 2007/0112948).

Since claims 11 and 50 depend from one of base claims 1 and 46, and include all of the limitations of the base claims, claims 11 and 50 should also be allowable over Geiger and Fransdonk. Further, Uhlik does not disclose any further limitations disclosed in the base claims. Therefore, claims 11 and 50 should be allowable over the combination of Geiger, Fransdonk, and Uhlik.

Accordingly, it is submitted that the rejection of claims 11 and 50 based upon 35 U.S.C. §103(a) has been overcome by the present remarks and withdrawal thereof is respectfully requested.

§103(a) Rejection of Claim 12

In Section 30 of the Office Action, claim 12 stands rejected under 35 U.S.C. 103(a) as being unpatentable over Geiger and Uhlik.

Since claim 12 depends from base claim 1, and includes all of the limitations of the base claim, claim 12 should also be allowable over Geiger and Uhlik.

Accordingly, it is submitted that the rejection of claim 12 based upon 35 U.S.C. §103(a) has been overcome by the present remarks and withdrawal thereof is respectfully requested.

§103(a) Rejection of Claims 8 and 14-17

In Section 32 of the Office Action, claims 8 and 14-17 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Geiger, as applied to Claim 1 above, and further in view of Abburi et al (U.S. Patent No. 7,203,966; hereinafter referred to as "Abburi").

Since claims 8 and 14-17 depend from base claim 1, and include all of the limitations of the base claim, claims 8 and 14-17 should also be allowable over Geiger. Further, Abburi does not disclose any further limitations disclosed in the base claim. Therefore, claims 8 and 14-17 should be allowable over the combination of Geiger and Abburi.

Accordingly, it is submitted that the rejection of claims 8 and 14-17 based upon 35 U.S.C. §103(a) has been overcome by the present remarks and withdrawal thereof is respectfully requested.

Conclusion

In view of the foregoing, applicants respectfully request reconsideration of claims 1, 3-5, 7-18, 20-23, 29, 31, and 46-50 in view of the remarks and submit that all pending claims are presently in condition for allowance.

In the event that additional cooperation in this case may be helpful to complete its prosecution, the Examiner is cordially invited to contact Applicant's representative at the telephone number written below.

Respectfully submitted,

Dated: 04/11/2011

By: /Samuel S. Lee/
Samuel S. Lee
Reg. No. 42,791

Procopio, Cory, Hargreaves & Savitch LLP
525 B Street, Suite 2200
San Diego, California 92101-4469
(619) 525-3821